

IN THE UNITED STATES DISTRICT COURT  
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF )  
INFORMATION ASSOCIATED WITH )  
VERIZON WIRELESS CELLULAR )  
TELEPHONE (424) 313-4713 THAT IS )  
STORED AT PREMISES CONTROLLED BY )  
VERIZON WIRELESS )

Mag. No. 16-1055

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Brett Massafra, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by Verizon Wireless, a wireless provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Verizon Wireless to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the cellular telephone number (424) 313-4713 (hereinafter the TARGET TELEPHONE) including the contents of communications.

2. I am a Trooper with the Pennsylvania State Police, employed by the Commonwealth of Pennsylvania. Your Affiant is currently assigned to the Bureau of Criminal Investigations, Drug Law Enforcement Division, Southwest Strike Force Unit, and I am responsible for illegal narcotics investigations. Your Affiant has been a Law Enforcement Officer for approximately 15 years, which includes being employed with the Donora Borough Police

Department from 2000 to June of 2008. While employed with the Donora Borough Police Department, your Affiant worked as a Detective with the Washington County District Attorney's Drug Task Force, where I was involved in undercover drug investigations. Also, while employed with the Donora Borough Police Department, I was assigned to work as a Task Force Officer with the Federal Bureau of Investigation's Mon Valley Resident Agency. While working as a Task Force Officer, I investigated Drug Trafficking organizations within the Mon Valley area, which includes Allegheny, Fayette, Washington, and Westmoreland Counties. Your Affiant has been a member of the Pennsylvania State Police since June 02, 2008, where I have been involved in undercover and special investigations for approximately six (6) years.

3. Your Affiant has received training at the Indiana University of Pennsylvania, Pennsylvania State Police Academy in Hershey, Pennsylvania, as well as basic and advanced illegal drug/narcotics investigation training conducted by the Pennsylvania State Police. Your Affiant has received extensive training relating to the enforcement of the Controlled Substance, Drug Device and Cosmetic Act and narcotics investigations from the from the Pennsylvania State Police, Traffic Institute for Police, Institute for Law Enforcement Education, Indiana University of Pennsylvania, North East Counter Drug Training Center, National Corrections and Law Enforcement Training and Technology Center, Drug Enforcement Agency, Federal Bureau of Investigation, and the Pennsylvania Office of the Attorney General. In addition, your Affiant has successfully completed TOP GUN training, which was an intensive training focused on undercover drug law enforcement operations and was instructed by the Pennsylvania State Police, the Pennsylvania Office of Attorney General and the Northeast Counterdrug Training Center in Harrisburg, Pennsylvania. Your Affiant has completed wiretapping and electronic surveillance training at the Pennsylvania State Police Bureau of Emergency and Special Operations, as

mandated in 18 Pa. C.S. § 5724, and, as a result, have received Class “A” certification (A-3772). This certification allows me to monitor and participate in court-authorized electronic surveillance.

4. Your Affiant, as a Trooper with the Pennsylvania State Police, Bureau of Criminal Investigations, and federal task force officer, is an “investigative or law enforcement officer” within the meaning of Section 5702 of the Pennsylvania Wiretapping and Electronic Surveillance Control Act, as well as an investigative or law enforcement officer of the United States within the meaning of Title 18, United States Code, Section 2510(7). During my career in law enforcement, I have planned, participated in, and supervised the execution of search warrants authorizing the search and seizure of drug traffickers, and locations associated with drug traffickers and their co-conspirators, such as residences, businesses, storage facilities, outbuildings, safety deposit boxes, and vehicles. I have been involved with numerous wiretap affidavits and investigations. I have written reports and analyzed documents in the course of investigations and testified in jury proceedings.

5. I have been involved in numerous post arrest interviews of individuals, interviewed defendants in conjunction with post-arrest proffers, and have interviewed confidential informants and other non-defendant individuals with knowledge of illegal drug trafficking. Through such interviews, as well as discussions with other experienced agents, I have become familiar with the day-to-day operations of both distributors and transporters of controlled substances. I have gained knowledge regarding the various methods, techniques, codes, and/or jargon used by illegal drug traffickers in the course of their criminal activities. For example, I have learned how they use firearms to protect their narcotics and about their use and patterns of communications using cellular telephones, and other telecommunication devices and applications, to facilitate communications while attempting to avoid law enforcement scrutiny. In addition, I have reviewed

thousands of communications between drug traffickers as a result of my participation in multiple wiretap investigations. As a result of my narcotics-related training and experience, I am familiar with the methods and language used to distribute narcotics, to launder proceeds, and to operate drug-trafficking conspiracies.

6. Based on my training and experience, I am aware that it is common practice for drug traffickers who desire to insulate themselves from detection by law enforcement to routinely utilize multiple telephones, counter surveillance, false or fictitious identities, and coded communications in order to communicate with their customers, suppliers, couriers, and other conspirators. It is not unusual for drug traffickers to initiate or subscribe such phone or phone device services under the names of other real or fictitious people. Moreover, it is now a very common practice for drug traffickers to utilize all communication features of their telephones, most notably the voice call and text message features, nearly simultaneously to communicate with their conspirators. For example, it is quite common for a particular transaction to be set up and completed using both voice calls and text messages. In fact, it is now quite unusual for a drug trafficker to utilize solely one feature of a telephone, such as the voice call feature, to further his criminal activities while not also using another feature, such as the text message feature, to further his criminal activities.

7. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

8. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 841, 843, and 846 have been committed by Jamie LIGHTFOOT and others known and unknown. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

### **PROBABLE CAUSE**

9. Your affiant is conducting an investigation into a drug trafficking organization involving Jamie LIGHTFOOT, who distributes cocaine in the area surrounding Donora, Pennsylvania, in the Western District of Pennsylvania. LIGHTFOOT is the user of the TARGET TELEPHONE, although it is subscribed to Update Info, 295 Parkshore Drive, Fulsome, CA 95630. I am aware that LIGHTFOOT is the user of the TARGET TELEPHONE in part because a Confidential Informant ("CI") has engaged in two controlled purchases of cocaine directly from LIGHTFOOT in which LIGHTFOOT used the TARGET TELEPHONE to arrange the transactions. The first of these controlled purchases involving the TARGET TELEPHONE was on July 5, 2016. The most recent of these controlled purchases was on October 27, 2016, when the CI ordered two ounces of cocaine in my presence, while speaking to LIGHTFOOT who was using the TARGET TELEPHONE. The CI and LIGHTFOOT then exchanged several text messages arranging to meet in person. I provided the CI with \$2,500 in official funds, searched his car to ensure that no controlled substances were present, and activated an audio recording device, which the CI wore on his person. Other troopers and I then conducted surveillance as LIGHTFOOT entered the CI's car. According to the CI and as confirmed by the audio recorder, the CI gave LIGHTFOOT the \$2,500 in official funds, and LIGHTFOOT gave the CI \$100 back and a knotted baggy containing a white powder. After LIGHTFOOT left the vehicle and the scene,

the CI met me at a predetermined location and gave me the \$100 and the bag of white powder, which field-tested positive for cocaine.

10. On November 1, 2016, based on the above information, I applied for a search warrant concerning the same information sought herein, which was granted the same day by Judge David Cashman of the Court of Common Pleas of Allegheny County, in the Commonwealth of Pennsylvania. The information returned from this search warrant included text messages, which I have shared with federal agents from the Federal Bureau of Investigation.

11. The text messages show that LIGHTFOOT communicates with other individuals who the CI has identified as local cocaine distributors. I believe that the CI is reliable because of his ability to conduct the controlled purchases described above. The messages show that LIGHTFOOT uses the TARGET TELEPHONE to meet with these individuals and conduct transactions, which I believe to be cocaine transaction based upon the controlled purchases described above. For example, on October 31, 2016, LIGHTFOOT ("JL") exchanged the following text messages with an individual I believe to be James Piatt ("JP"), using telephone number (724) 503-0962, which is subscribed to James Piatt:

JL: Yo im ready for u but u have to start knocking that bill u owe me now

JP: I'm going to I'm going to get this lil bit off and I'm trying to come wit a couple stacks jay I can't remember where would that put us at

JL: We at 3300

JP: We can just rap about it when I come down

JL: Ok

12. In my training and experience, I know that it is common for drug traffickers to “front” drugs to lower-level distributors, meaning allow them to take drugs to sell while promising to pay for the drugs later. This results in situations like the one reflected above, in which LIGHTFOOT references “that bill u owe me now” and Piatt “can’t remember where would that put us,” which I interpret to mean that Piatt is unsure how much he owes LIGHTFOOT for cocaine. LIGHTFOOT’s response “3300” suggests that Piatt owes LIGHTFOOT \$3,300, which is an amount consistent with the purchase of two-ounce quantities of cocaine for \$2,400, as discussed above.

13. In combination, the facts describe above provide probable cause that LIGHTFOOT uses the TARGET TELEPHONE to arrange and conduct cocaine transactions, and that evidence of his violations of 21 U.S.C. §§ 841, 843, and 846 will be found within the information requested herein.

14. In my training and experience, I have learned that Verizon Wireless is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, and multimedia messages for Verizon Wireless subscribers may be located on the computers of Verizon Wireless. Further, I am aware that computers located at Verizon Wireless contain information and other stored electronic communications belonging to unrelated third parties.

15. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of Verizon Wireless for weeks or months.

16. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by Verizon Wireless for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

17. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

18. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded



unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEIN”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

19. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which “cell towers” (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question. In addition to the authority cited above, I request this information under 18 U.S.C. § 2703(d), because this affidavit provides “specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.” In particular, the information showing the “cell towers” with which the TARGET TELEPHONE has connected will show the approximate location of the TARGET TELEPHONE during cocaine transactions, which will then improve agents’ ability to identify LIGHTFOOT’s cocaine customers and associates, as well help reveal his source of cocaine supply. Your affiant is aware that LIGHTFOOT recently traveled to New York State, and I suspect that the trip was to meet with a cocaine supplier. Cell site location information will help determined whether LIGHTFOOT makes the same trip regularly, in a manner that would suggest the existence of a New York supplier.

20. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

21. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

22. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is

analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This “timeline” information may tend to either inculcate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device’s owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner’s motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

23. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Verizon Wireless to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B.

Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

### **CONCLUSION**

24. Based on the forgoing, I request that the Court issue the proposed search warrant.

25. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that – has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i). The controlled purchase described above occurred within the Western District of Pennsylvania.

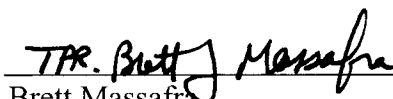
26. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

27. The United States further requests that the Order require Verizon Wireless not to notify any person, including the subscriber or customer of the account listed in Attachment A, of the existence of the Order until further order of the Court. See 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue “an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order.” *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order will seriously jeopardize the investigation, including by giving

targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. See 18 U.S.C. § 2705(b)(2), (3), (5). Some of the evidence in this investigation is stored electronically. If alerted to the investigation, the subjects under investigation could destroy that evidence, including information saved to their personal computers.

28. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

  
Brett Massafra  
Trooper  
Pennsylvania State Police

Subscribed and sworn to before me on November 10, 2016

  
CHIEF UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with **(424) 313-4713** that is stored at premises owned, maintained, controlled, or operated by Verizon Wireless, a wireless provider headquartered at 180 Washington Valley Road, Bedminster, New Jersey 07921

**ATTACHMENT B**

**Particular Things to be Seized**

**I. Information to be disclosed by Verizon Wireless**

To the extent that the information described in Attachment A is within the possession, custody, or control of Verizon Wireless, including any messages, records, files, logs, or information that have been deleted but are still available to Verizon Wireless or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Verizon Wireless is required to disclose the following information to the government for each account or identifier listed in Attachment A:

- a. All voice mail, text, and multimedia messages stored and presently contained in, or on behalf of the account or identifier;
- b. All existing printouts from original storage of all of the text messages described above;
- c. All transactional information of all activity of the telephones and/or voicemail accounts described above, including log files, messaging logs, local and long distance telephone connection records, records of session times and durations, dates and times of connecting, methods of connecting, telephone numbers associated with outgoing and incoming calls, all data about which “cell towers” (i.e., antenna towers covering specific geographic areas) and “sectors” (i.e., faces of the towers) received a radio signal from each cellular telephone or device assigned to the Accounts, to include non-contemporaneous cell site location information for the Accounts, and a

listing of all cell sites and control channels and the physical address of each cell site for the areas in which the Accounts are operating; and/or locations used from July 5, 2016 to present;

d. All text messaging logs, including date and time of messages, and identification numbers associated with the handsets sending and receiving the message;

e. All business records and subscriber information, in any form kept, pertaining to the individual accounts and/or identifiers described above, including subscribers' full names, addresses, shipping addresses, date account was opened, length of service, the types of service utilized, ESN (Electronic Serial Number) or other unique identifier for the wireless device associated with the account, Social Security number, date of birth, telephone numbers, and other identifiers associated with the account;

f. Detailed billing records, showing all billable calls including outgoing digits, from July 5, 2016 to present;

g. All payment information, including dates and times of payments and means and source of payment (including any credit or bank account number), from July 5, 2016 to present;

h. Incoming and outgoing telephone numbers, from July 5, 2016 to present;

i. All records indicating the services available to subscribers of individual accounts and/or identifiers described above;

j. All records pertaining to communications between Verizon Wireless and any person regarding the account or identifier, including contacts with support services and records of actions taken.

## **II. Information to be seized by the government**



All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 21 U.S.C. §§ 841, 843, and 846 involving Jamie LIGHTFOOT since July 5, 2016, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- (a) The distribution of illegal drugs, including cocaine;
- (b) Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;
- (c) Evidence indicating the geographic location of the cellular device at times relevant to the investigation;
- (d) Evidence indicating the cellular device owner or user's state of mind as it relates to the crime under investigation;
- (e) The identity of the person(s) who created the account associated with the cellular device and/or used the cellular device, including records that help reveal the whereabouts of such person(s).
- (f) The identity of the person(s) who sent to and/or received communications from the cellular device about matters relating to illegal drug trafficking, including records that help reveal their whereabouts.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC**  
**BUSINESS RECORDS PURSUANT TO FEDERAL RULE**  
**OF EVIDENCE 902(11)**

I, \_\_\_\_\_, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Verizon Wireless, and my official title is \_\_\_\_\_. I am a custodian of records for Verizon Wireless. I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Verizon Wireless, and that I am the custodian of the attached records consisting of \_\_\_\_\_ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Verizon Wireless; and

c. such records were made by Verizon Wireless as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature